MISSION & OBJECTIVES

The National Computer Forensics Institute (NCFI) is dedicated to the education of law enforcement professionals in the field of computer forensics and digital evidence handling techniques.

The NCFI includes five high-tech classrooms, a mock courtroom, a computer forensic lab, and other meeting and training areas. The NCFI will support both cyber crime and computer forensic training for state and local law enforcement, prosecutors and judges from across the country.

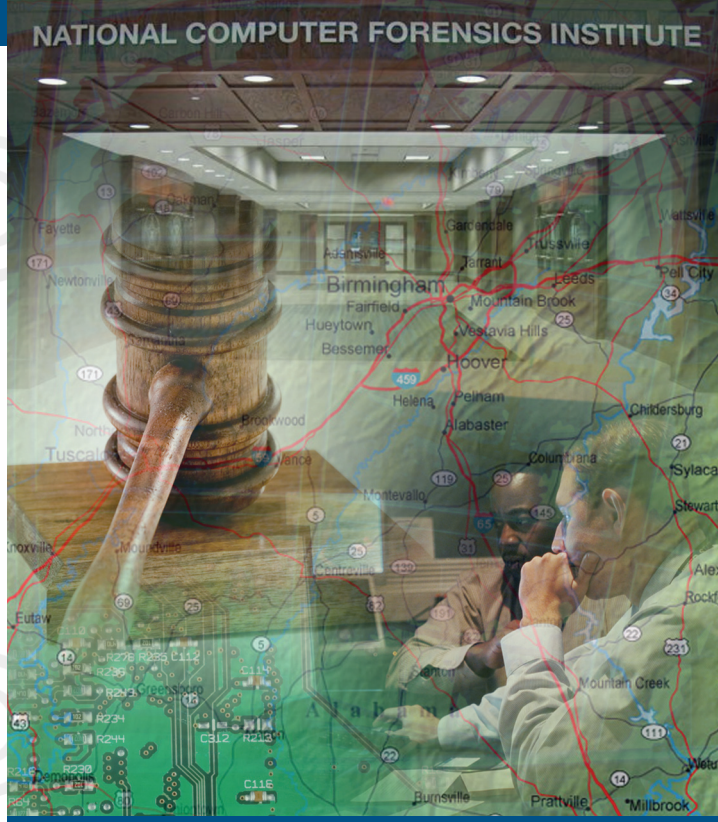
Today's high-tech environment presents new challenges to law enforcement as cyber criminals exploit computers and the Internet to threaten our banking, financial and critical infrastructures. Therefore, it is imperative to address the changes in technology by providing training on cyber-investigative techniques and by sharing current expertise.

For further information, please contact the *National Computer Forensics Institute* at the following:

National Computer Forensics Institute
2020 Valleydale Road, Suite 209
Hoover, AL 35244

Tel. 205/989-5300 • Fax 205/989-5305

www.ncfi.usss.gov



NCFI

National Computer Forensics Institute

Hoover, Alabama

U.S. Department of Homeland Security

United States Secret Service

OVERVIEW & HISTORY

The National Computer Forensics Institute (NCFI) was established in 2007 through a partnership initiative between the Department of Homeland Security, the United States Secret Service, the Alabama District Attorneys Association, the State of Alabama, and the city of Hoover. This state-of-the-art facility will provide state and local law enforcement officers the training necessary to conduct basic electronic crimes investigations, respond to network intrusion incidents, and conduct computer forensics examinations.

This facility offers state and local law enforcement officers, prosecutors, and judges a variety of cyber related courses based on the Secret Service electronic crimes training model. All NCFI training courses are made available through funding from the Department of Homeland Security. All travel, lodging, and per diem expenses are paid by the Department of Homeland Security and courses are provided at no costs to attendees. Upon completion of training, attendees are issued all computer equipment, hardware, software, manuals, and tools necessary to conduct electronic crimes investigations and forensic examinations.

This innovative facility and strategic partnership will substantially enhance law enforcement efforts to suppress the continually evolving and increasing number of electronic crime cases affecting communities nationwide.

COURSES OFFERED

BICEP
Basic Investigation of Computer and Electronic Crimes Program
This is a five-day course designed to provide investigators with the ability to act as a first responder to a variety of cyber related cases.

NITRO
Network Intrusion Response Program
This fourteen day course is designed to provide training on how to effectively respond to a network incident including mitigation of the problem, collecting volatile data, and fully investigating a network based crime.

BCERT
Basic Computer Evidence Recovery Training
This is a five-week course designed to provide hands-on experience with computer hardware, device imaging solutions, forensic analysis tools, legal issues and report generation for law enforcement officers performing as cyber incident responders and digital evidence examiners.

ACERT
Advanced Computer Evidence Recovery Training
This is a five-day course designed to provide experienced forensic examiners with the knowledge and abilities to apply network /server based forensics processing skills.

CFC-J
Computer Forensics in Court - Judges
This four-day course provides hands-on experience with computer and networking technology to allow judges to obtain knowledge and insight into presiding over criminal cases involving digital evidence.

CFC-P
Computer Forensics in Court - Prosecutors
This five-day course provides hands-on experience with computer and networking technology to allow prosecutors to obtain knowledge and insight into handling criminal cases involving digital evidence.